Security & Privacy Policy from an Enterprise Perspective

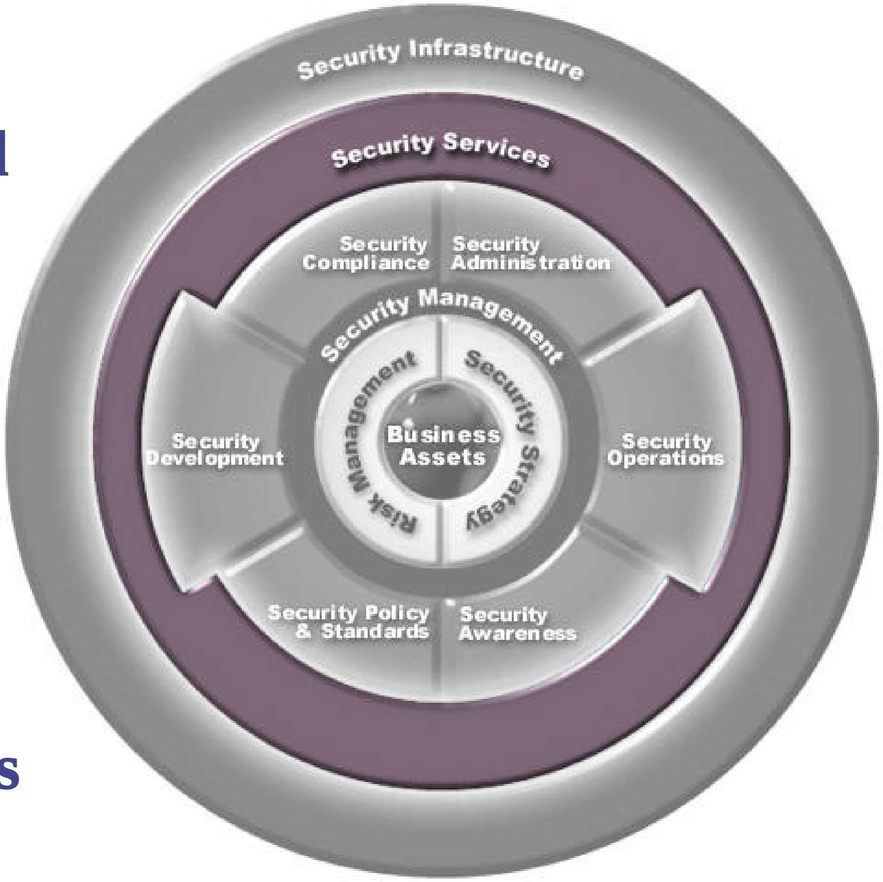
Andy Boots

Champion for

Information Security & Privacy

Security Services Envelope

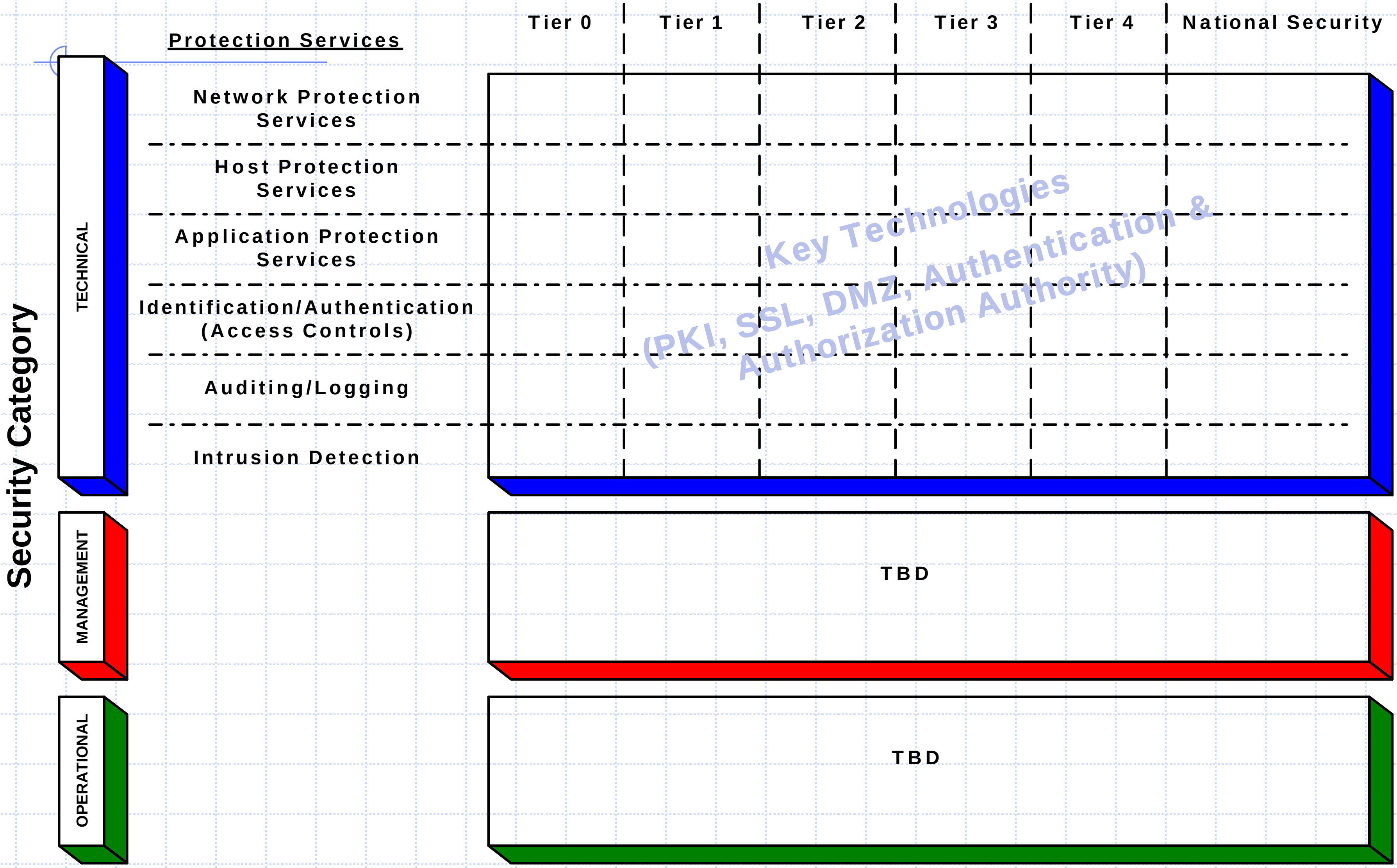
- Consistency and standards in architecture
- Central administration and operations
- Shared development resources
- Reduced cost
- Increased speed of deployment
- Higher security due to fewer solutions and systems for similar requirements



Security Services Layer

- *Security Services* are re-useable common security architecture components which have been documented and packaged to allow easy re-deployment.
- The objective of the *Security Services Layer* is to achieve consistency and standardization across the enterprise for common security functions such as identification, authentication, authorization, accountability, integrity, and confidentiality.

Security Protection Services Framework



Certification Tier

Tier 0

Tier 1

Tier 2

Tier 3

Tier 4

National Security

Protection Services

Security Category

TECHNICAL

Network Protection Services

Host Protection Services

Application Protection Services

Identification/Authentication (Access Controls)

Auditing/Logging

Intrusion Detection

Key Technologies (PKI, SSL, DMZ, Authentication & Authorization Authority)

MANAGEMENT

TBD

OPERATIONAL

TBD

Zachmann Security Force-Fit

Perspective/ Model	Data	Business Function	Network	People	Schedule	Motivation/Strategy
Planner/Scope	• Students • Information Exchange – FFEL Community – Schools – Lenders/Partners • Employees • Laws/Executive Orders	• Access Controls • Application and System Software Controls • Entity-wide Security Controls • Continuity of Business Operations • System Security Certification & Accreditation • Risk Abatement	• Virtual Data Center • FSA Remote Users • ASPs • FSA Regional Offices • EDI	• Office of the CIO • Ed Cyber Security Organization • GSA FEDCIRC • FBI NIPC • Other External Security Organizations • Other Internal Security Organizations • Segregation of Duties	• Response to New Security Law, Regulation, or Executive Order • Identification of new: – Students – Financial Partners – Lenders	• Achieve & Preserve Information Security – Satisfy Existing Laws and Executive Orders Relating to Information Assurance – Cyber Security Capital Planning
Owner/Business Model	• ED Enterprise – Networks – Applications – Hosts • Business Entities & Relationships – Channels – FFEL • Information Classification	• Process Flow diagrams for the above • Secure and Reliable Information Exchange • Process Classification • GISRA Audits • Security Training • Security Monitoring	• FSA Data Networks Mapping – Data Link – Network • FSA Distributed System Architecture • System Classification	• Security Management Framework – Organization Structure, CONOPS, and Work Products of Cyber Security Organization – Organization Structure, CONOPS, and Work Products of CIRC Organization • ISO Process and Procedures • Trust Model/Relationships	• C&A Life Cycle – Security Definition – Budget – Verification – Validation – Post Accreditation	• Cyber Security Organization Business Plan – Core Security Principles – Cyber Security Goals and Objectives – ED Security Directives – SSO Strategy – Threat Assessment
Designer/System Model	• Security Technical Architecture Handbook • Security Standards Profile – Schools Security Standards – Student Loan Industry Security Standards			• Cyber Security Operations Guide • Permissions Model for System/Information Read/Write/Create/Delete • Security Monitoring – Network – Host – Applications	• System Security Engineering Processes • Security Processes & Plans, e.g. – Security Incident Response Process – Technology Refresh Process – Business Continuity Plan – Disaster Recovery Plan	• FSA SSO Guidance/ Handbooks • System Security Plan • Risk Assessment
	• FSA Security Methods – Confidentiality – Integrity – Availability	• System Diagrams for all of the above • Functional Specifications for all of the above • Security Controls Specifications	• Defense-in-Depth Layers • Design documents for – Network View – Host View – Application View			
Builder/ Technology Model	• Data storage, interchange, & reporting standards for security incidents and intrusion detection	• PKI • Identification & Authentication Process • Access Control Process • Non-repudiation Process • Malicious Code Detection & Containment • Alerting • Audit Log Processing • Backup Processing	• Selected technologies for – Encryption/VPN – Firewalls – Access – App. Security	• Procedures Manuals – Firewall Reconfiguration – System Security Audits – Forensic Analysis • Crew Position Training, Certification, and Operators Manuals	• Subprocesses for the above, e.g. – Event Response Procedures – PKI RA Processes & Procedures	• Availability & Performance Objectives • Best Security Practices, e.g. – PIN Policy – PKI Certificate Policy
Subcontractor/ Components	• System Component Security Databases	• Detailed Inventory of Security HW/SW Components, Configurations, Versions	• Detailed Location and Connectivity of HW/SW Inventory	• Positive Identification/ Authentication of Individuals and their role	• Steps for the above, e.g. – SDLC Activity Checklists	• System Certification and Accreditation • Position Certification Requirements

Security & Privacy Threats Fall into Three Categories -- CIA

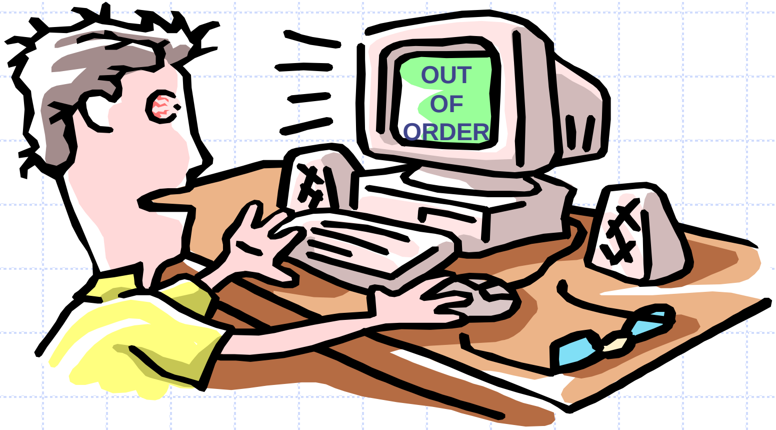
CONFIDENTIALITY

Information must be protected from unauthorized disclosure

INTEGRITY

Data must be reliable, therefore accurate

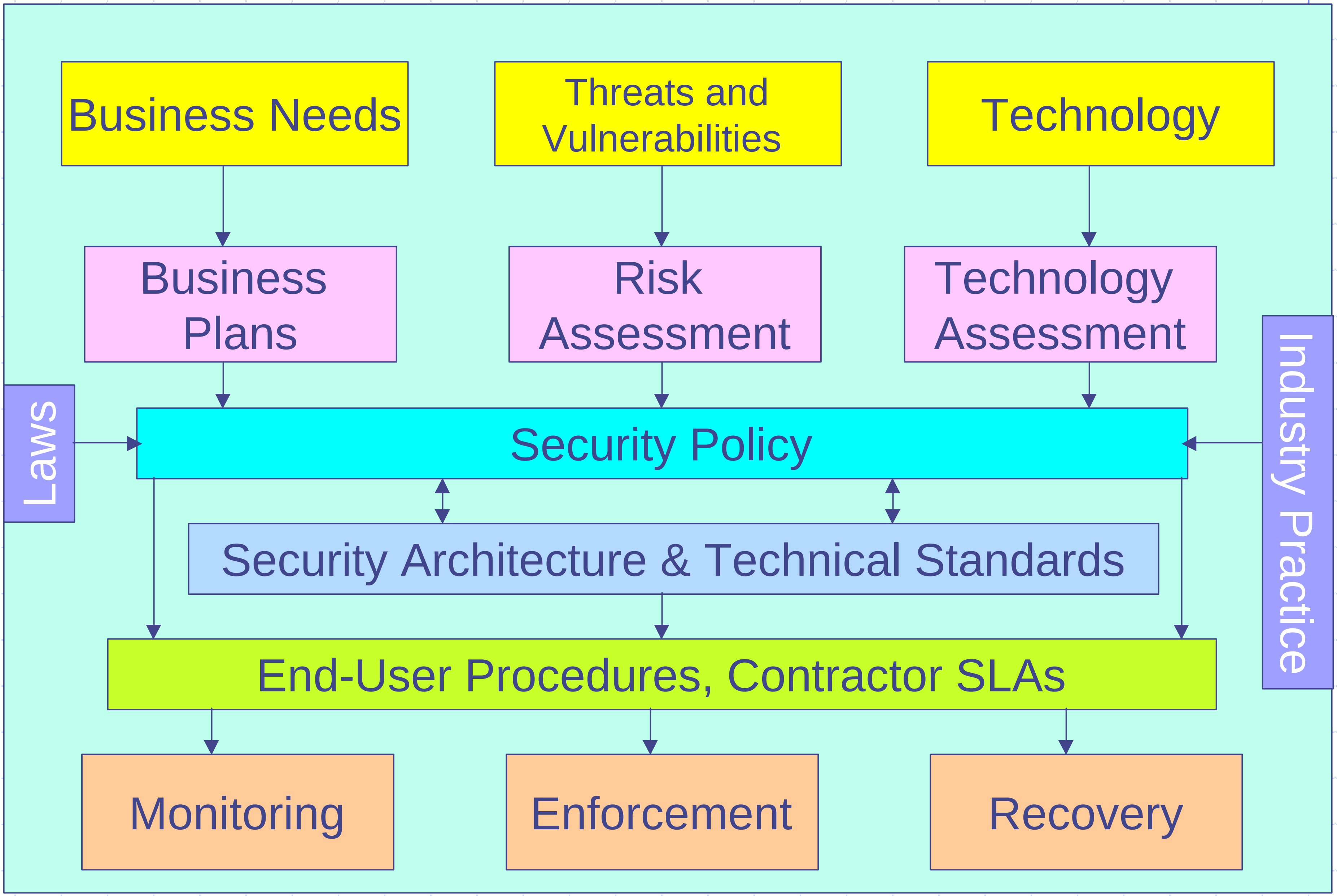
AVAILABILITY



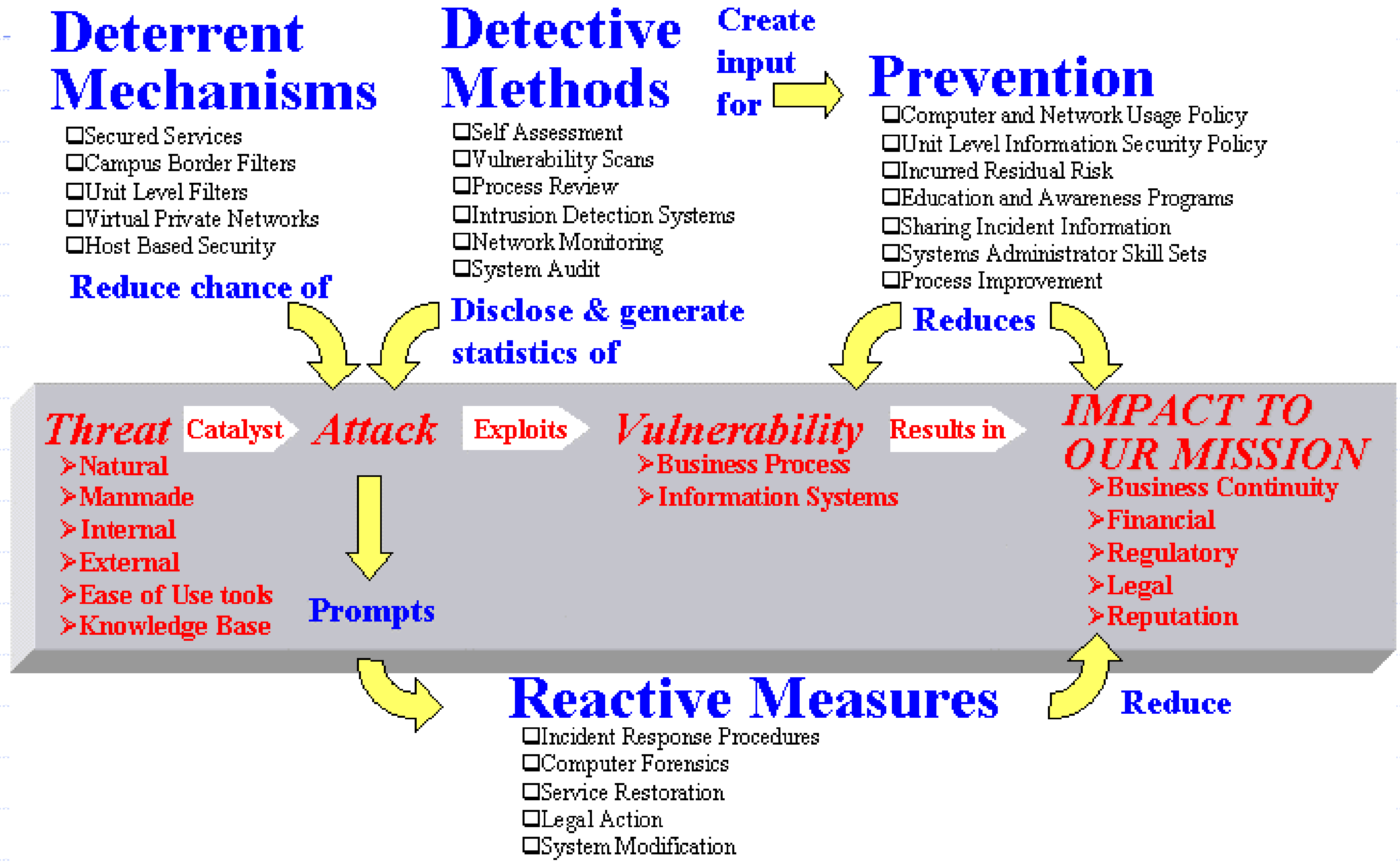
Information & systems must be accessible when needed

+ Accountability

Security Vision and Strategy



Security Architecture Overview



Deterrent Mechanisms

- ❑Secured Services
- ❑Campus Border Filters
- ❑Unit Level Filters
- ❑Virtual Private Networks
- ❑Host Based Security

Reduce chance of

Detective Methods

- ❑Self Assessment
- ❑Vulnerability Scans
- ❑Process Review
- ❑Intrusion Detection Systems
- ❑Network Monitoring
- ❑System Audit

Disclose & generate statistics of

Create input for

Prevention

- ❑Computer and Network Usage Policy
- ❑Unit Level Information Security Policy
- ❑Incurred Residual Risk
- ❑Education and Awareness Programs
- ❑Sharing Incident Information
- ❑Systems Administrator Skill Sets
- ❑Process Improvement

Reduces

Threat Catalyst *Attack* Exploits *Vulnerability* Results in *IMPACT TO OUR MISSION*

Threat
- ➢Natural
- ➢Manmade
- ➢Internal
- ➢External
- ➢Ease of Use tools
- ➢Knowledge Base

Vulnerability
- ➢Business Process
- ➢Information Systems

IMPACT TO OUR MISSION
- ➢Business Continuity
- ➢Financial
- ➢Regulatory
- ➢Legal
- ➢Reputation

Prompts

Reactive Measures

- ❑Incident Response Procedures
- ❑Computer Forensics
- ❑Service Restoration
- ❑Legal Action
- ❑System Modification

Reduce

SFA'S SECURITY/PRIVACY CONTEXT

Congress

- Privacy Act of 1984
- Computer Security Act of 1987
- Paperwork Reduction Act of 1990
- Government Performance & Results Act of 1993
- Clinger-Cohen Act of 1996
- Government Information Security Reform Act of 2000

Executive Branch

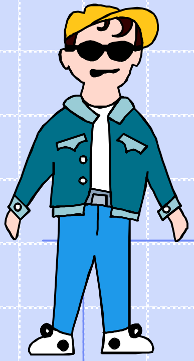
- OMB Circular A-130, Appendix III
- NIST Guidance (800 Series)

Department of Education

- Computer Security Officer Handbook
- Information Technology Security Plan

SFA

- Security & Privacy Policies
- Risk Assessments
- Personnel Screening
- System Security Plans
- Security Training
- Incident Response
- Certification & Accreditation
- Security in SLC
- Security Awareness
- Intrusion Detection
- Penetration Testing

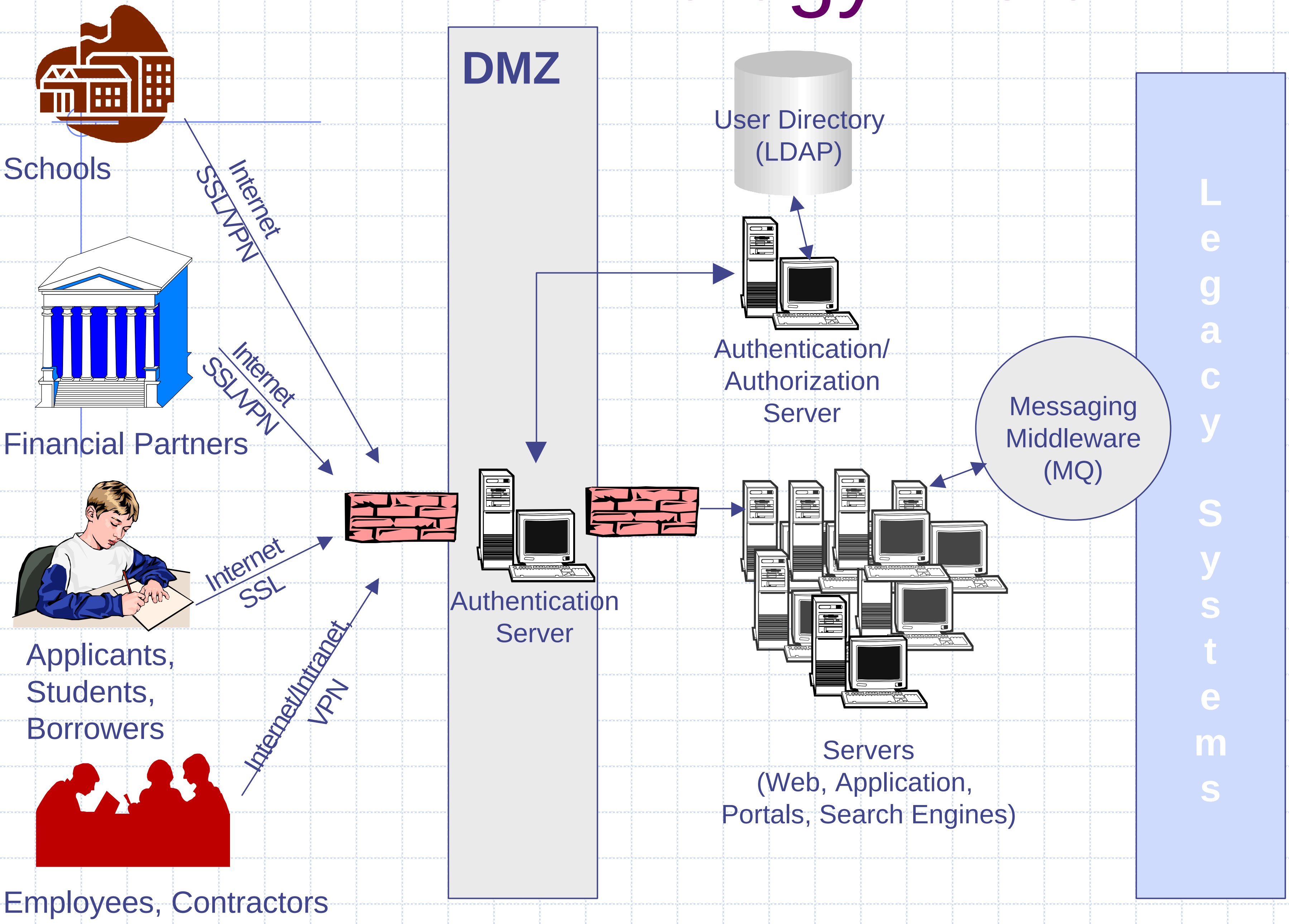


Identification: Of all the people I know, which are you?

Authentication: How can I be sure you are who you say you are?

Authorization: OK, if that's who you are, what can you do in my system?

E-ID Technology Vision



Schools

Internet SSL/VPN

Financial Partners

Internet SSL/VPN

Applicants, Students, Borrowers

Internet SSL

Employees, Contractors

Internet/Intranet, VPN

DMZ

Authentication Server

User Directory (LDAP)

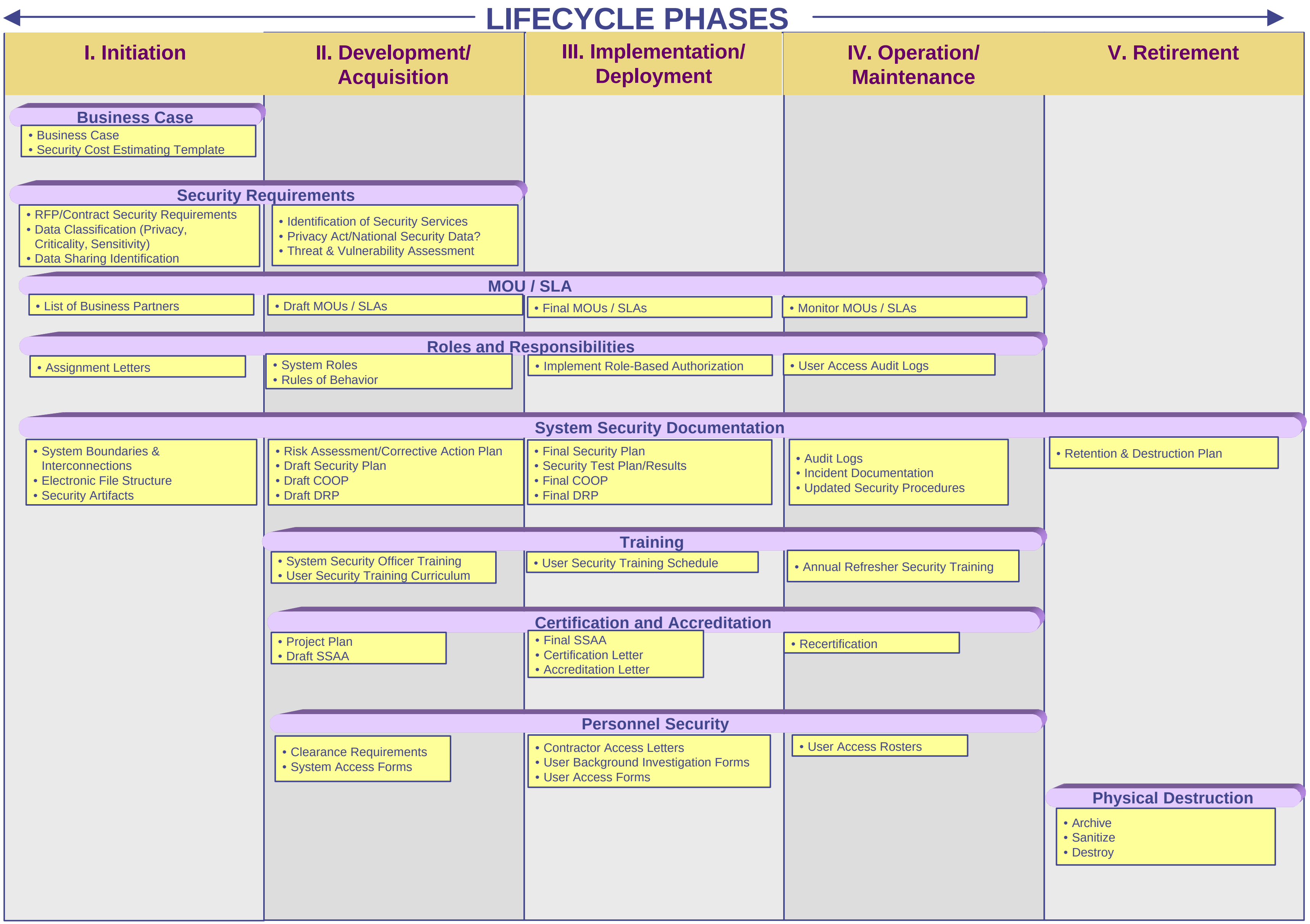
Authentication/ Authorization Server

Messaging Middleware (MQ)

Servers (Web, Application, Portals, Search Engines)

Legacy Systems

(Required Products)



LIFECYCLE PHASES

	I. Initiation	II. Development/ Acquisition	III. Implementation/ Deployment	IV. Operation/ Maintenance	V. Retirement
Business Case	• Business Case • Security Cost Estimating Template				
Security Requirements	• RFP/Contract Security Requirements • Data Classification (Privacy, Criticality, Sensitivity) • Data Sharing Identification	• Identification of Security Services • Privacy Act/National Security Data? • Threat & Vulnerability Assessment			
MOU / SLA	• List of Business Partners	• Draft MOUs / SLAs	• Final MOUs / SLAs	• Monitor MOUs / SLAs	
Roles and Responsibilities	• Assignment Letters	• System Roles • Rules of Behavior	• Implement Role-Based Authorization	• User Access Audit Logs	
System Security Documentation	• System Boundaries & Interconnections • Electronic File Structure • Security Artifacts	• Risk Assessment/Corrective Action Plan • Draft Security Plan • Draft COOP • Draft DRP	• Final Security Plan • Security Test Plan/Results • Final COOP • Final DRP	• Audit Logs • Incident Documentation • Updated Security Procedures	• Retention & Destruction Plan
Training		• System Security Officer Training • User Security Training Curriculum	• User Security Training Schedule	• Annual Refresher Security Training	
Certification and Accreditation		• Project Plan • Draft SSAA	• Final SSAA • Certification Letter • Accreditation Letter	• Recertification	
Personnel Security		• Clearance Requirements • System Access Forms	• Contractor Access Letters • User Background Investigation Forms • User Access Forms	• User Access Rosters	
Physical Destruction					• Archive • Sanitize • Destroy